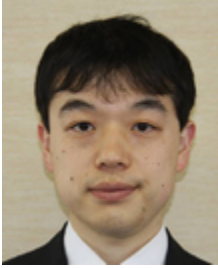


Information Security Laboratory



Yodai Watanabe
Senior Associate Professor



Akihito Nakamura
Senior Associate Professor



Yen Neil Yuwen
Associate Professor



Chunhua Su
Associate Professor



Li Zhenni
Visiting Researcher

Refereed academic journal

[chsu-103-002-01:2017] Yamin Wen Weijie Li-Zheng Gong Lu Zhou, Chunhua Su. Towards practical white-box lightweight block cipher implementations for IoTs. *Future Generation Computer Systems*, 86:507–514, September 2018.

According to the Kerckhoffs's principle, the security of a system should be only depended on the security of its secret key. To build the trusted computing base, Secure Element (SE) and Trusted Execution Environment (TEE) have been proposed for secure computing and authentication. But users still need to believe that SE and TEE-supported hardware will not be evil or intruded. In order to totally remove the dependence of extra hardware, white-box cryptography was introduced by Chow et al. (2002) which gives a software solution for AES implementations in an extremely hostile environment. After Chow et al.'s seminal paper, many white-box implementations were proposed on different block ciphers. In IoTs applications, SE and TEE might have the practical issues if the implementation costs are constrained. In this paper, we first discuss the practical issues that relate to white-box block cipher implementations from lightweight block ciphers. Furthermore, we give the white-box implementations of KLEIN, Present and LBlock as the typical candidates that represent the Substitution-Permutation Network (SPN) and Feistel structures. Finally the performance and the costs are compared with the white-box AES implementation. The comparison shows that white-box implementations are not only related to block and key lengths, but also the structure of the cipher and its white-box implementation methodology strongly affect the implementation costs.

[chsu-103-002-02:2017] Chunhua Su Lam For Kwok Wenjuan Li, Weizhi Meng. Towards False Alarm Reduction Using Fuzzy If-Then Rules for Medical Cyber Physical Systems. *IEEE Access*, 6:6530 – 6539, January 2018.

Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical processes. Its process control is often referred to as embedded systems. Generally, CPS and Internet of Things have the same basic architecture, whereas the former shows a higher combination and coordination between physical and computational elements, i.e., wireless sensor networks can be a vital part of CPS applications. With the rapid development, CPS has been applied to healthcare industry, where a wide range of medical sensors are used within a healthcare organization. However, these sensors may generate a large number of false alarms in practice, which could significantly reduce the system effectiveness. Targeting

on this issue, in this work, we attempt to design a Medical Fuzzy Alarm Filter (named MFASFilter) for healthcare environments by means of fuzzy logic, especially fuzzy if-then rules, which could handle the vague and imprecise among data. In the evaluation, we conducted two major experiments to explore the performance of our approach in a simulated and a real network environment, respectively. Experimental results demonstrate that the use of fuzzy if-then rules could achieve a better accuracy as compared to the traditional supervised algorithms, and that our designed filter is effective in the practical environment.

[chsu-103-002-03:2017] Kuo-Hui Yeh Zijia Huang Chunhua Su Shi-Cho Cha, Ming-Shiung Chuang. A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices. *IEEE Access*, (6):20779–20787, March 2018.

The deployment of IoT devices with significant data collection capabilities around the world raises concerns about user privacy. People are worried about ubiquitous IoT devices collecting and sharing their data with unknown parties without their awareness or consent. Currently, several governmental agencies have stated that IoT service providers should obtain user consent before collecting and using their personal data. However, to the best of our knowledge, there is no standard means for users to reach agreements on privacy practices for IoT applications. Among different types of IoT applications, this paper focuses on the scenario in which people use their personal smartphones to access nearby IoT devices via Bluetooth Low Energy (BLE). To address the privacy issue in the scenario, this paper proposes a privacy preferences expression framework for BLE-based applications named PrivacyBat. The framework defines specifications for users to achieve agreements on privacy practices with nearby BLE devices. In addition, this framework provides guidelines for a device to process user requests according to the agreement. To demonstrate how the framework operates, this paper further provides a proof of concept implementation. As the proposed framework can improve the privacy policy agreement process in IoT applications, this paper can hopefully contribute to increasing user trust in IoT applications.

[chsu-103-002-04:2017] Chunhua Su Jianying Zhou Rongxing Lu Weizhi Meng, Wenjuan Li. Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data. *IEEE Access*, 6:7234 – 7243, November 2017.

Internet of Things (IoT) has been widely used in our daily life, which enables various objects to be interconnected for data exchange, including physical de-

Summary of Achievement

vices, vehicles, and other items embedded with network connectivity. Wireless sensor network (WSN) is a vital application of IoT, providing many kinds of information among sensors, whereas such network is vulnerable to a wide range of attacks, especially insider attacks, due to its natural environment and inherent unreliable transmission. To safeguard its security, intrusion detection systems (IDSs) are widely adopted in a WSN to defend against insider attacks through implementing proper trustbased mechanisms. However, in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, we focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure. In the evaluation, we investigate the performance of our approach in both a simulated and a real network environment. Experimental results demonstrate that packet-based trust management would become ineffective in a heavy traffic environment, and that our approach can help lighten the burden of IDSs in handling traffic while maintaining the detection of insider attacks

[chsu-103-002-05:2017] Chunhua Su Kuo-Hui Yeh Shi-Cho Cha, Jyun-Fu Chen. A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. *IEEE Access*, 6:24639–24649, January 2018.

Recently, the popularity of the Internet of Things (IoT) has led to a rapid development and significant advancement of ubiquitous applications seamlessly integrated within our daily life. Owing to the accompanying growth of the importance of privacy, a great deal of attention has focused on the issues of secure management and robust access control of IoT devices. In this paper, we propose the design of a blockchain connected gateway which adaptively and securely maintains user privacy preferences for IoT devices in the blockchain network. Individual privacy leakage can be prevented because the gateway effectively protects users' sensitive data from being accessed without their consent. A robust digital signature mechanism is proposed for the purposes of authentication and secure management of privacy preferences. Furthermore, we adopt the blockchain network as the underlying architecture of data processing and maintenance to resolve privacy disputes.

[chsu-103-002-06:2017] Xin Sun Xishun Zhao Kim-Kwang Raymond Choo Lu Zhou, Chunhua Su. Stag hunt and trust emergence in social networks. *Future Generation Computer Systems*, 88:168–172, November 2018.

Trust plays an important role in interactions within complex social systems.

In this paper, we use multi-agent learning to study trust emergence in social networks. In our setting, agents play an iterative game of Stag Hunt with their neighbors. An agent adopts the learning rule imitate-the-best to learn how to play the game. Trust emerges if all agents choose to hunt stag after repeated play of the Stag Hunt game. We study the probability of the emergence of trust among agents living in different social networks. Using experiments, we reveal critical points of trust emergence in lattice network, ring network and small world model. The probability of trust emergence is relatively low if the quotient of the value of trust and the basic utility is smaller than the critical point. The probability, however, grows quickly when the quotient is larger than the critical point. In scale-free networks, there is no such critical point. Our findings also demonstrate that on scale-free networks, trust emerges only if the value of trust is several times larger than the basic utility.

[chsu-103-002-07:2017] Wayne Chiu Lu Zhou Kuo-Hui Yeh, Chunhua Su. I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics. *IEEE Communications Magazine*, 56(2):150–157, February 2018.

The comprehensive evolution of information communication technologies on mobile sensing objects has led to the provision of versatile ubiquitous network services embedded with specific- purpose modern sensors and intelligent wearable devices. The universal Internet connectivity of such smart objects has brought about a new era of ubiquitous application development for the Internet of Things. Meanwhile, security has become critically important. In the past decade, academia and industry have dedicated great efforts to the design of continuous authentication for multi-modal networks. Multifactor authentication bio-tokens have been introduced for continuous entity identification and verification. With the rapid growth and universality of wearable devices, in this article we target continuous authentication for the IoT-based environment with users possessing wearable healthcare (and wellness) related smart objects. To present the state of the art, we provide a comprehensive review of continuous authentication in recent years. Critical characteristics of new biometrics are then introduced. Second, we present a wearable plantar bio-feature extractor constructed via commercial pressure sensors and the Raspberry PI platform. The prototype is adopted to retrieve user plantar bio-data as the raw (and training) data in the proposed authentication system. Third, we apply machinelearning- based techniques to derive a user’s plantar bio-features as authentication tokens in the system to support continual (and real-time) entity verification in the background without the user’s notice.

Summary of Achievement

[chsu-103-002-08:2017] Gerhard P. Hancke Zhe Liu Chunhua Su Lu Zhou, Kuo-Hui Yeh. Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints. *IEEE Signal Processing Magazine*, 35(5):76 – 87, September 2018.

Endpoint devices form a core part of the architecture of the Industrial Internet of Things (IIoT). Aspects of endpoint device security also extend to related technology paradigms, such as cyberphysical systems (CPSs), edge computing, and fog computing. In this sphere, there have been several initiatives to define and promote safer and more secure IIoT networks, with the Industrial Internet Consortium (IIC) and OpenFog Consortium having developed security framework specifications detailing the techniques and technologies to secure industrial endpoints.

[chsu-103-002-09:2017] Atsuko Miyaji Chunhua Su Jiageng Chen, Rashed Mazumder. Variable message encryption through blockcipher compression function. *Concurrency and Computation: Practice and Experience*, 29(7), Mach 2017.

A constrained device is an emerging technology that has enormous applications in our daily life such as access control, inventory control, luggage tracking, barcode reader, and IoT. However, it has certain drawbacks of low memory and less computing power. Thus, one of the cracking challenges is to provide efficient and secure cryptographic solution for the constrained device in the aspect of security issue. An (n,n) blockcipher-based cryptographic compression function is applicable to provide provable security to the constrained device. Though, there are many constructions of (n,n) blockcipher such as MDC2, MDC4, MJH, Bart12, and SKS15. However, most of the familiar schemes are not suitable for short and variable message encryption without padding because of their internal structures. Furthermore, the security margin is provided based on blocklength rather than the flexible size of message. In this paper, we present two different (n,n) blockcipher compression function schemes. The first scheme (FS) satisfies better efficiency such as less call of blockcipher, less key scheduling, and higher efficiency rate. On the contrary, the second scheme (SS) has upper security bound. Moreover, both of the schemes are suitable for small and variable message encryption, which is handy for the constrained device. The collision and preimage security bound of the FS are $O(2tn/2)$ and $O(2tn)$. In addition, the SS's collision resistance and preimage resistance are bounded by $O(2tn)$ and $O(22tn)$. Moreover, the efficiency rate of the proposed two schemes are respectively t and $t/3$. The numbers of key scheduling are 2 for the constructions of

FS and SS. We use two calls of blockcipher in the FS. On the contrary, three calls of blockcipher are used in the SS.

[chsu-103-002-10:2017] Chunhua Su Rashed Mazumder, Atsuko Miyaji. A simple authentication encryption scheme. *Concurrency and Computation: Practice and Experience*, 29(16), February 2017.

n authentication encryption (AE) scheme satisfies to transfer an authenticated data between 2 parties or more. There are vast applications of the AE such as access control, encryption, enhancing trust between multiple parties, and assure the originality of a message. However, the main challenge of the AE is to maintain low-cost features for its construction. Furthermore, there is another emerging issue of Internet of Things (IoT) in the field of data and network communication. The numbers of application of the IoT are increasing expeditiously, where various kinds of device have been used such as IoT-end device, constrained device, and RFID. Moreover, the main challenge of the IoT-end devices and resource constrained devices is to keep a certain level of security bound including minimum cost. However, the IoT-end devices, resource constrained devices, and RFID have lack of resources such as memory, power, and processors. Interestingly, the AE can play a vital role between data acquisition (sensors, actuators) and data aggregation of usual platform of the IoT. Thus, the construction of the AE should satisfy the properties of low-cost, least resources, and less operating time. Though, there are many familiar constructions of AE such as OTR, McOE, POE, OAE, APE, COPE, CLOC, and SILK but most of the schemes depend on the features of nonce and associate data. In the aspect of security, the usage of nonce and associated data are adequate. However, these 2 features increase the overhead cost. Therefore, we propose a simple construction of IV-based AE where blockcipher compression function is used as encryption function. Our proposed scheme's efficiency-rate is 1 with reasonable privacy security bound. In addition, it can encrypt arbitrary length of message in each iteration without padding.

[chsu-103-002-11:2017] Chunhua Su Rashed Mazumder, Atsuko Miyaji. Free Access Probably Secure Keyed-Function Based Authenticated Encryption Schemes for Big Data. *International Journal of Foundations of Computer Science*, 28(6), September 2017.

Security, privacy and data integrity are the critical issues in Big Data application of IoT-enable environment and cloud-based services. There are many upcoming challenges to establish secure computations for Big Data applications. Authenticated encryption (AE) plays one of the core roles for Big Data's confidentiality,

Summary of Achievement

integrity, and real-time security. However, many proposals exist in the research area of authenticated encryption. Generally, there are two concepts of nonce respect and nonce reuse under the security notion of the AE. However, recent studies show that nonce reuse needs to sacrifice security bound of the AE. In this paper, we consider nonce respect scheme and probabilistic encryption scheme which are more efficient and suitable for big data applications. Both schemes are based on keyed function. Our first scheme (FS) operates in parallel mode whose security is based on nonce respect and supports associated data. Furthermore, it needs less call of functions/block-cipher. On the contrary, our second scheme is based on probabilistic encryption. It is expected to be a light solution because of weaker security model construction. Moreover, both schemes satisfy reasonable privacy security bound.

[chsu-103-002-12:2017] Kim-Kwang Raymond Choo Wayne Chiu Kuo-Hui Yeh, Chunhua Su. A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things. *Sensors*, 17(5), May 2017.

Rapid advances in wireless communications and pervasive computing technologies have resulted in increasing interest and popularity of Internet-of-Things (IoT) architecture, ubiquitously providing intelligence and convenience to our daily life. In IoT-based network environments, smart objects are embedded everywhere as ubiquitous things connected in a pervasive manner. Ensuring security for interactions between these smart things is significantly more important, and a topic of ongoing interest. In this paper, we present a certificateless signature scheme for smart objects in IoT-based pervasive computing environments. We evaluate the utility of the proposed scheme in IoT-oriented testbeds, i.e., Arduino Uno and Raspberry PI 2. Experiment results present the practicability of the proposed scheme. Moreover, we revisit the scheme of Wang et al. (2015), and revealed that a malicious super type I adversary can easily forge a legitimate signature to cheat any receiver as he/she wishes in the scheme. The superiority of the proposed certificateless signature scheme over relevant studies is demonstrated in terms of the summarized security and performance comparisons.

[nakamura-103-002-01:2017] Kikuchi S., Watanabe S., Kenmotsu T., Yoshino D., Nakamura A., and Hayashi T. Analysis of Impactful Factors on Performance in Combining Architectural Elements of IoT. *Advances in Internet of Things (AIT)*, 7(4):121–138, Oct 2017.

We implemented a generalized infrastructure for Internet of Things (IoT infrastructure) to be applicable in various areas such as Smart Grid. That IoT infrastructure has two methods to store sensor data. They commonly have the

features of double overlay structure, virtualization of sensors, composite services as federation using publisher/subscriber. And they are implemented as synthesizing the elemental architectures. The two methods majorly have the common architectural elements, however there are differences in how to compose and utilize them. But we observed the non-negligible differences in their achieved performance by the actual implementations due to operational items beyond these architectural elements. In this paper, we present the results of our analysis about the factors of the revealed differences based on the measured performance. In particular, it is clarified that a negative side effect due to combining independent elemental micro solutions naively could be amplified, if maximizing the level of loose coupling is applied as the most prioritized design and operational policy. Primarily, these combinations should be evaluated and verified during the basic design phase. However, the variation of how to synthesize them tends to be a blind spot when adopting the multiple independent architectural elements commonly. As a practical suggestion from this case, the emphasized importance in carrying out a new synthetization with multiple architectures is to make a balance naturally among architectural elements, or solutions based on them, and there is a certain demand to establish a methodology for architectural synthetization, including verification.

[neilyyen-103-002-01:2017] Neil Y. Yen Guangli Zhu Shunxiang Zhang, Shiyao Zhang. The Recommendation System of Micro-Blog Topic Based on User Clustering. *Mobile Networks and Applications*, 22(2):228–239, 2017.

As a type of crowdsensing media, micro-blog has become an important crowdsensing place for a lot of real-time information dissemination and discussion. With the increasing of micro-blog users, there are more and more new topics emerging on this kind of platform, which has made the users difficult in finding out their own interesting topics. To solve this problem, this paper proposes a micro-blog topic recommendation system which can give corresponding suggestions/strategies for users. Firstly, the user relationship (i.e., a user adds a follow hyperlink to another user) in micro-blog can be effectively analyzed and saved to the user graph. In addition, an algorithm of computing user authority (which is similar to the idea of PageRank) is proposed to catch influential users based on the built user graph. Secondly, Topic Feature Graph (TFG) and User Micro-blog Feature Graph (UMFG) are respectively constructed based on the micro-blog text corpus of a topic and the micro-blog texts followed by a given user. Based on TFG and UMFG, User Topic Feature Vector (UTFV) and User Topic Fea-

Summary of Achievement

ture Matrix (UTFM) can be achieved. After that, users' similarity is calculated based on the User Topic Feature Vector and User Topic Feature Matrix to realize the users clustering by the help of the hierarchical clustering algorithm. Incorporating topic heat degree and user authority, the recommendation algorithm is presented to realize Micro-blog topic personalized recommendation within user clustering set. Experiments show that our proposed recommendation system has a good accuracy which is up to 50.2 %.

[neilyyen-103-002-02:2017] Neil Y. Yen Moloud Abdar. Design of A Universal User Model for Dynamic Crowd Preference Sensing and Decision-Making Behavior Analysis. *IEEE ACCESS*, 5:24842–24852, 2017.

Sharing economy becomes an emerging issue in urban life. It is not a new phenomenon but an assembling of existing techniques to meet specific demands of users. It also points out a better way to implicitly collect users' contexts and to understand users than the conventional one that requires much user involvement (e.g., tedious inputs). A universal model, for this purpose, that supports dynamic analysis and mining of user-generated content (or contexts) is designed in this paper. Two major factors, sensing and analysis of crowd preference and their decision-making behavior, are especially targeted. This model formulates the given scenario that comprehensively illustrates the possible actors and correlated actions among them with a set of rules to enhance the machine learning results. This model outlines a detail process on pre-/post-process of the data, and indicates the core techniques for user modeling. The raw data collected from on-service website, i.e., Airbnb, are utilized for the preliminary examination of our proposal. We especially look at internal factors (e.g., nationality, gender, and age) and external factors (e.g., device, social media, and time) that reflect implicitly the difference on crowd's preference and behavior. Results after statistics-based machine learning reveal that the relation among users' internal and external factors share high similarity with their behavior patterns, and can be applied, considering particular features, for service provision to a specific type of crowds.

[neilyyen-103-002-03:2017] Zhihan Lu Kim-Kwang Raymond Choo Lin Mei Xi-angfeng Luo Zheng Xu, Neil Y. Yen. Social Media Based Online Attention Computing of Public Security Events. *IEEE Transactions on Emerging Topics in Computing*, 5(3):403–411, 2017.

Nowadays, the probability of public safety events around the world increase quickly. Recently, with the development of mobile network and intelligent mobile phones, social media users play an important role of the evolution and

management of a public safety event. One of the important functions of Weibo is to monitor real time public safety events, such as fire, explosion, traffic jam, etc. Weibo users can be seen as social sensors and Weibo can be seen as the sensor platform. In this paper, a crowdsensing based online attention computing method of public safety events is proposed. The proposed method contains three steps. First, a mobile crowdsensing based social media crawler is given. Second, spatial and temporal information is used to analyze the online attention of the public safety event. At last, the proposed model based online attention governance system is given. The system collected the online attention data from Weibo. Besides, given the Weibo posts related to a detected public safety event, the proposed method targets at mining the multi-modal information, as well as storytelling the online attention of the public safety event precisely and concisely. Extensive experiment studies on real-world microblog datasets to demonstrate the superiority of the proposed framework. Case studies on real data sets show the proposed model has good performance and high effectiveness in the analysis of public safety events.

[neilyyen-103-002-04:2017] Neil Y. Yen Moloud Abdar. Understanding Regional Characteristics through Crowd Preference and Confidence Mining in P2P Accommodation Rental Service. *Library Hi Tech*, 35(4):521–541, 2017.

Purpose This research intends to look at the regional characteristics through an analysis of crowd preference and confidence, and investigates how regional characteristics are going to affect human beings at all aspects in a scenario of sharing economy. The purpose of this paper is to introduce an approach to provide an understandable rating score. Furthermore, the paper aims to find the relationships between different features classified in this study by using machine learning methods. Furthermore, due to the importance of performance of methods, the performance of the features is also improved. **Design/methodology/approach** The Rating Matching Rate (RMRate) approach is proposed to provide score in terms of simplicity and understandability for all features. The relationships between features can be extracted from accommodation data set using decision tree (DT) algorithms (J48, HoeffdingTree, and REPTree). Usability of these methods was evaluated using different metrics. Two techniques, “ClassBalancer” and “SpreadSubsample,” are applied to improve the performance of algorithms. **Findings** Experimental outcomes using the RMRate approach show that the scores are very easy to understand. Three property types are very popular almost in all of selected countries in this study (“apartment”, “house”, and “bed and breakfast”). The findings also indicate that “Entire home/apt” is the most

Summary of Achievement

common room-type and 4.5 and 5 star-rating are the most given star-rating by users. The proposed DT algorithms can find the relationships between features significantly. In addition, applied CB and SS techniques could improve the performance of algorithms efficiently. Originality/value This study gives precise details about the guests' preferences and hosts' preferences. The proposed techniques can effectively improve the performance in predicting the behavior of users in sharing economy. The findings can also help group decision making in P2P platforms efficiently.

[neilyyen-103-002-05:2017] Neil Y. Yen Heng Lee, Moloud Abdar. Event-based trend factor analysis based on hashtag correlation and temporal information mining. *Applied Soft Computing*, 71:1204–1215, 2018.

Nowadays, using social media such as Twitter, Facebook, etc., has become extremely popular among individuals around the world. Utilizing various event analysis algorithms for research on which event/events is/are the hottest as well as discovering the reason(s) behind it/them. Based on our proposed model, we can investigate about all of the reasons of the events and why they triggered the event(s) to a comprehensive discussions. In addition, we can list the reason's impact from the highest one to the lowest one. The idea of event-based analysis is that we can access a good explanation on social interactions and behaviors associated with complex situations. Previous studies can be simply categorized into two parts. One part is the discovery of event clusters with different temporal concerns, and the other part is the collection of related event(s) and the calculation of correlated connection strength among them. But both parts are only focused on the lack of notice the reason why these events have been discussed. Our proposed model is searching for the deeper issue, not only the idea behind the event, but also the reason why it makes the event triggered the comprehensive discussion. Furthermore, different from the clustering algorithm, our search layer can be increased as many as we need until reaching the goal. We demonstrate our model for constructing a strength table that contains the reasons related to the event, and the result can be presented precisely either as a table or a graph for user's easy-understanding.

[neilyyen-103-002-06:2017] Yunhuai Liu Chuanping Hu-Lin Mei Neil Y. Yen Kim-Kwang Raymond Choo Vijayan Sugumaran Zheng Xu, Xiangfeng Luo. From Latency, through Outbreak, to Decline: Detecting Different States of Emergency Events Using Web Resources. *IEEE Transactions on Big Data*, 4(2):245–257, 2018.

An emergency event is a sudden, urgent, usually unexpected incident or occur-

rence that requires an immediate reaction or assistance for emergency situations, which plays an increasingly important role in the global economy and in our daily lives. Recently, the web is becoming an important event information provider and repository due to its real-time, open, and dynamic features. In this paper, web resources based states detecting algorithm of an event is developed in order to let the people know of an emergency event clearly and help the social group or government process the emergency events effectively. The relationship between web and emergency events is first introduced, which is the foundation of using web resources to detect the state of emergency events imaged on the web. Second, five temporal features of emergency events are developed to provide the basis for state detection. Moreover, the outbreak power and the fluctuation power are presented to integrate the above temporal features for measuring the different states of an emergency event. Using these two powers, an automatic state detecting algorithm for emergency events is proposed. In addition, heuristic rules for detecting the states of emergency event on the web are discussed. Our evaluations using real-world data sets demonstrate the utility of the proposed algorithm, in terms of performance and effectiveness in the analysis of emergency events.

[yodai-103-002-01:2017] Manami Sasaki and Yodai Watanabe. Visual Secret Sharing Schemes Encrypting Multiple Images. *IEEE Transactions on Information Forensics and Security*, 13(2):356–365, 2018.

The aim of this work is to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images. First, the formulation of access structures for a single secret is generalized to that for multiple secrets. This generalization is maximal in the sense that the generalized formulation makes no restrictions on access structures; in particular, it includes the existing ones as special cases. Next, a sufficient condition to be satisfied by the encryption of VSS schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of VSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate VSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. Moreover, for threshold access structures, the pixel expansions of VSS schemes generated by the latter construction are estimated and turn out to be the same as those of the existing schemes called the threshold multiple-secret visual cryptographic schemes (MVCS). Finally, the optimality of the former construction is examined, giving that there exist access

Summary of Achievement

structures for which it generates no optimal VSS schemes.

Refereed proceedings of an academic conference

[chsu-103-002-13:2017] Lijun Jiang Zhe Liu Chunhua Su Jinguang Han Weizhi Meng, Fei Fei. CPMaP: Design of Click-Points Map-Based Graphical Password Authentication. In Lech Jan Janczewski Mirosław Kutylowski, editor, *SEC: IFIP International Conference on ICT Systems Security and Privacy Protection*, 2018.

As traditional textual passwords suffer from many known limitations, graphical passwords (GPs) are proposed as one promising alternative to complement the existing authentication systems. To obtain a large password space, map-based GPs (geographical passwords) have been developed that allow users to choose one or more places on a map for authentication. For example, PassMap requires users to choose two places as their credentials, and GeoPass enables users to click only one place for authentication. Some research studies have reported that choosing only one place as a password may be not secure enough, whereas selecting two places may decrease the system usability. In this work, we first conducted a study to learn how users would choose two places under PassMap, and found that users may choose two similar locations due to time consideration. Motivated by this observation, we then design CPMaP, a click-points map-based GP scheme that allows users to choose one place on a world map at first and then click a point or an object on an image relating to the previously selected location. To investigate the performance of CPMaP, we conducted another user study with up to 50 participants. It is found that users could achieve promising results with our scheme in the aspects of both security and usability.

[nakamura-103-002-02:2017] Watanabe S. and Nakamura A. Integrated Data Access to Heterogeneous Data Stores for IoT Cloud. In Sieminski A. et al., editor, *Modern Approaches for Intelligent Information and Database Systems, Studies in Computational Intelligence Vol. 769*. Springer, 2018.

Recently, Internet of Things (IoT) attract attention. The authors are developing a cloud platform for IoT applications. The IoT cloud needs to deal with various types of data and large data sets depending on applications and purpose of use. That is, the IoT cloud necessarily includes heterogeneous data stores in a mixed manner. For example, relational databases and NoSQL databases have different connection methods and query languages. This configuration complicates the

system design and increases the development cost. This paper presents a configuration method of data access component (DAC) that absorbs the connection method and the query language differences among data stores. This allows us to develop IoT applications without worrying about data store differences and later replacements. In the implementation, we used specific DACs optimized for specific data stores and a multi-purpose DAC Apache MetaModel. With a large scale data set of more than one million records under most configurations, the response time for various kinds of queries are less than 1 second.

Unrefereed proceedings of an academic conference

[nakamura-103-002-03:2017] Sato Y., Fujii Y., and Nakamura A. Development of Health Care Applications using Personal Data Store. In *IPSJ SIG Technical Report, 2018-GN-104*, March 2018.

With the rapid advances in AI and IoT technologies, personal data became valuable resources to society and business. Vendor Relationship Management (VRM) is an activity which aims to provide customers with control of personal data and independence from vendors. A software tool called PDS (Personal Data Store) realizes VRM. Although VRM and PDS are factors that are important in personal data utilization, they have not become common. We are proceeding with the research of PDS technology by developing applications in the field of health care. The objectives are definitions of the functional requirements and the external interfaces of PDS. In this paper, we present user cases and applications which utilize health care data and PDS. We use an open source PDS, Personium, for implementation. The base system collects user's health care data via wearable devices and stores them in PDS. The applications assist user's effort to promote good health by visualization of health care data and automatic reminding. The prototype confirmed that PDS facilitates implementation of self-information control rights and data portability requirements demanded by VRM.

[nakamura-103-002-04:2017] Nochi T. and Nakamura A. Network Simulator for IoT. In *IPSJ 80th National Convention*, March 2018.

[nakamura-103-002-05:2017] Kokubun Y. and Nakamura A. Analysis of Malicious URLs on Social Networking Services and Protection. In *Society of Socio-Informatics (SSI) Annual Meeting*, September 2017.

Summary of Achievement

Cyber attack is one of the most serious threats facing many organizations in the Internet era. In addition to hardening computer and network systems, it is important to surely deliver security information to end users. This paper presents the results of analysis on malicious messages and URLs sent on a social networking service; Twitter. We also present a method and system for safe-browsing of URL links. URLs, and sometimes shortened URLs, on SNS may be utilized for malicious activities to redirect users to unexpected resources, e.g. phishing and malware, by obscuring the final destinations. The analysis results show that about 20 percent of messages contain at least one URL, 0.1 percent of messages contain malicious URLs. The users sent such messages and messages themselves have short lifetime on Twitter. That is, they are removed soon after malicious activities; 99 percent of them are disappeared within one month. The proposed system enables users to know how safe a particular Web resource might be before users dereference it. Our system retrieves and delivers safety information of the URLs on user's demand by a simple operation.

Research grants from scientific research funds and public organizations

[chsu-103-002-14:2017] Chunhua Su. Information Security Framework for Wearable Devices, 2018-2020.

[chsu-103-002-15:2017] Chunhua Su Yaokai Feng Kouichi Sakurai, Hiroaki Anada. Systematic Evaluation on Security and Privacy of Crypto-Virtual Currency, 2018-2020.

[chsu-103-002-16:2017] Masakazu Soshi Atsuko Miyaji, Chunhua Su. New Lightweight Cryptosystems for IoT devices and application to eHealth Environments in Taiwan, 2015-2019.

[chsu-103-002-17:2017] Chunhua Su. Authentication and Privacy-preserving technologies for IoT-enable Environment, 2015-2017.

[yodai-103-002-02:2017] Yodai Watanabe. JSPS Grant-in-Aid for Scientific Research (C), 2015-2018.

Academic society activities

[chsu-103-002-18:2017] Hiroaki Kikuchi Chunhua Su, September 2018.

Program co-chair of The 14th International Conference on Information Security Practice and Experience (ISPEC 2018)

[neilyyen-103-002-07:2017] Steering Chair, The 6th IET International Conference on Frontier Computing

Advisor for undergraduate research and graduate research

[yodai-103-002-03:2017] Yuto Miura. Master Thesis: Numerical Experiments to Estimate Security of Audio Secret Sharing Schemes Encrypting Audio Secrets, University of Aizu, 2017.

Thesis Advisor: Y. Watanabe

[yodai-103-002-04:2017] Jumpei Otsuka. Graduation Thesis: Modification of the Integer Factorization by Number Field Sieve, University of Aizu, 2017.

Thesis Advisor: Y. Watanabe

[yodai-103-002-05:2017] Takumi Tabe. Graduation Thesis: Analysis of the Distributions of Dissimilarity Distance Based on Compression, University of Aizu, 2017.

Thesis Advisor: Y. Watanabe

[yodai-103-002-06:2017] Ryosuke Kawakubo. Graduation Thesis: Simple Formulation of Structural Similarity for Halftoning, University of Aizu, 2017.

Thesis Advisor: Y. Watanabe

Others

[yodai-103-002-07:2017] Ryosuke Kawakubo. Simple Formulation of Structural Similarity for Halftoning, 2017.

2017 IPSJ Tohoku Section Student Award

[yodai-103-002-08:2017] Takumi Tabe. Analysis of the Distributions of Dissimilarity Distance Based on Compression, 2017.

2017 IEEJ Tohoku Section Student Award

Summary of Achievement

Contributions related to syllabus preparation

[nakamura-103-002-06:2017] CSC01 Information Security

[nakamura-103-002-07:2017] L06 Information Security

Scholarly paper prepared by undergraduate/graduate student(s) you advised

[yodai-103-002-09:2017] Manami Sasaki and Yodai Watanabe. Visual Secret Sharing Schemes Encrypting Multiple Images. *IEEE Transactions on Information Forensics and Security*, 13(2):356–365, 2018.

Contribution related to student management (for example, solution of a student-related problem)

[chsu-103-002-19:2017] class mentor

Contribution related to the building or operation of the university computer system

[nakamura-103-002-08:2017] ISTC Steering Committee, member

Contribution related to planning administration for research, research conferences, or international research

[neilyyen-103-002-08:2017] Committee member, SGU Committee Group 2 (com2), 2017

[neilyyen-103-002-09:2017] Committee member, SGU Committee Group 2 (com2), 2018

[neilyyen-103-002-10:2017] Person-in-charge, Chaoyang University of Technology, Taiwan

[neilyyen-103-002-11:2017] Person-in-charge, Tamkang Technology, Taiwan

[neilyyen-103-002-12:2017] Person-in-charge, National Chi-Nan University, Taiwan

Contribution related to educational research technology and facility planning management

[nakamura-103-002-09:2017] Revitalization Center Steering Committee, member

Other significant contribution toward university planning, management, or administration

[neilyyen-103-002-13:2017] Committee member, Health and Welfare Guidance Committee, 2017

[neilyyen-103-002-14:2017] Committee member, Health and Welfare Guidance Committee, 2018

Contributions related to regional education

[nakamura-103-002-10:2017] Cyber Security Trends, lecture at Fukushima Prefecture Police, April 2017

[nakamura-103-002-11:2017] Cyber Security Trends, lecture at Fukushima Prefecture Police School, September 2017

Proposal/implementation of a new industry

[nakamura-103-002-12:2017] Secure Cloud Computing, presentation and exhibition at Industry, Academia, Government, Finance, Collaboration Fair 2018 in Miyagi, January 2018

Contribution toward education for employees of regional industries

[nakamura-103-002-13:2017] Cyber Security Seminar for Business Leaders, Aizu, November 2017 and Koriyama, December 2017

[nakamura-103-002-14:2017] Cyber Security Seminar and Drill for IT Professionals, Aizu, January 2018

Summary of Achievement

**Did you participate in Public Lectures, and/or Open Campus?
(Yes or No) If yes, please describe what you did.**

[nakamura-103-002-15:2017] Information Security, open lecture, Aizu Keikodo, August 2017

[nakamura-103-002-16:2017] Building Secure Computing Environment, open labs, August 2017

[nakamura-103-002-17:2017] Building Secure Computing Environment, open labs, October 2017

[yodai-103-002-10:2017] Open Laboratory at Open Campus 2017 (Summer and Autumn Sessions)